U.S. DEPARTMENT OF ENERGY | Nuclear Energy

Cyber Security R&D (NE-1) and (NEET-4)

Trevor Cook

Office of Science and Technology Innovation

Office of Nuclear Energy
U.S. Department of Energy

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Cyber Security for Nuclear Systems (the threat is real)

- July 2014 - China Hacks Canadian National Research Council
- March 2014 – China Hacks OPM
- 2011-2014 – Russian Cyber attacks against U.S. Energy Companies
- January 2013 – Department of Energy Hacked
- October 2011 - China Hacks Iron Dome (Israel's missile defense)

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Regulatory Framework for Cyber Security

- **10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks"**
  - requires licensees to protect digital computer and communications systems and networks associated with the following categories of functions, from those cyber attacks identified in 10 CFR 73.54(a)(2):
    - safety-related and important-to-safety functions
    - security functions
    - emergency preparedness functions, including offsite communications, and
    - support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

- **Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities"**
  - Guidance for meeting 10 CFR 73.54

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

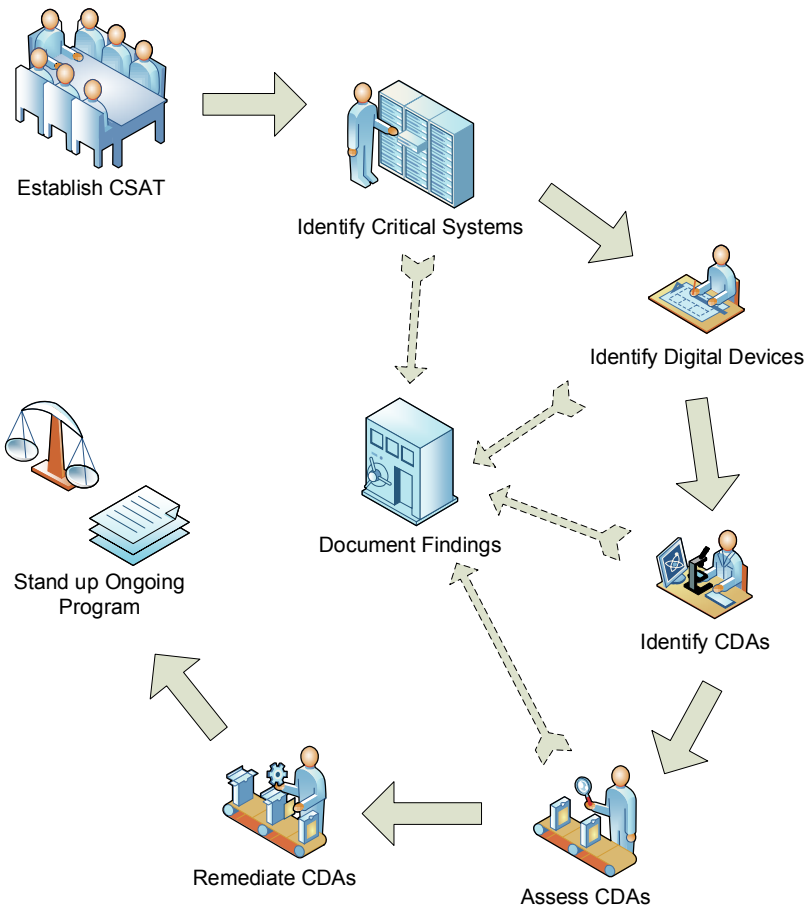
Regulatory Framework for Cyber Security

- **Regulatory Guide 1.152, Rev. 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"**
  - guidance for establishing a "Secure Development and Operational Environment (SDOE)"
  - endorses provisions of IEEE Standard 7-4.3.2-2003

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Implementing Cyber Security

Establish Cyber Security Assessment Team



Implement Portable and Mobile Device Controls

Identify Critical Systems and Critical Digital Assets

Implement ongoing program for Cyber Security

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Purpose of Cyber Security R&D

- To reduce the vulnerability
- To mitigate the consequence
- To lower the costs
- To provide a partner

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Sample Cyber Security R&D Needs

Cyber-hardened Sensors and Networks

- Technologies and methodologies to assure secure sensors, networks and communication systems
- Technologies and methodologies to test the security of sensors, networks and communication systems

Modeling and Simulation

- Methodologies to apply nuclear simulation codes to evaluate the consequences of cyber attacks
- Experiments to validate such methods
- Risk based methodologies for prioritizing vulnerabilities

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Sample Cyber Security R&D Needs

- **Personnel Protection Systems and Insider Threat**
  - Technologies and methodologies needed to measure security effectiveness, predict emerging threat risk trends and predict security performance anomalies that may increase personnel and their private systems' exposure to cyber targeting

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

NEET vs NEUP

- **NEET seeks broadly applicable nuclear sector R&D**
  - Develop a methodology to resolve consequences from cyber attacks
  - Demonstrate an application of the methodology
- **NEUP seeks Research Reactor specific R&D**
  - Identify a potential vulnerability
  - Conduct analyses and/or experiments to evaluate the vulnerability
  - Use lessons learned in the curriculum
- **Awards are not intended to assist with regulatory compliance issues**

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Contact Information

- For NEET and NEUP, interested parties may contact the INL cyber security program manager at steven.harenstein@inl.gov
- Interested parties may contact me as well at trevor.cook@nuclear.energy.gov